مدخل الى

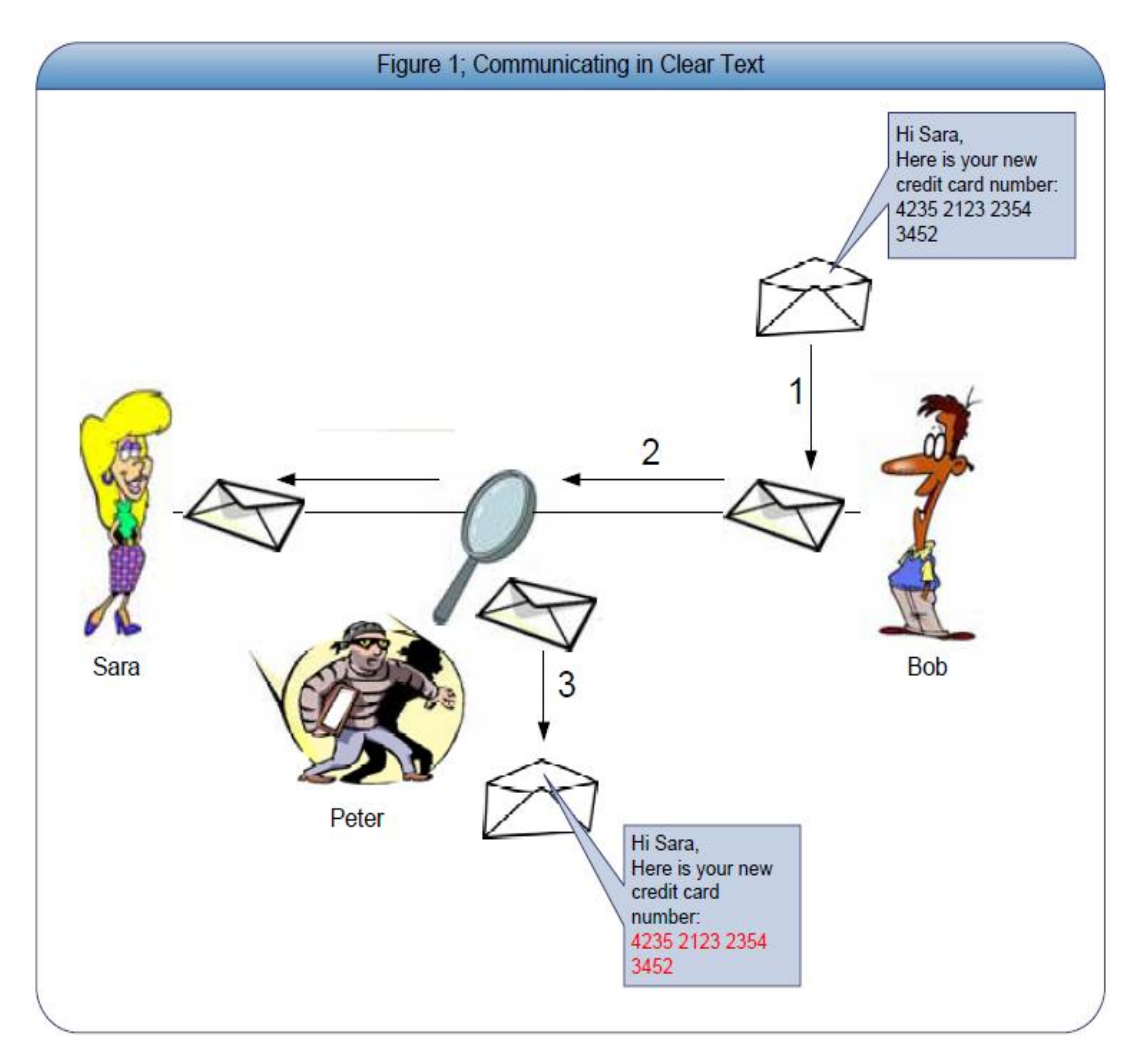
علم التشفير (التعمية)

النسخة العربية : المهندس : محمد عبد الفتاح على قايد – اليمن –

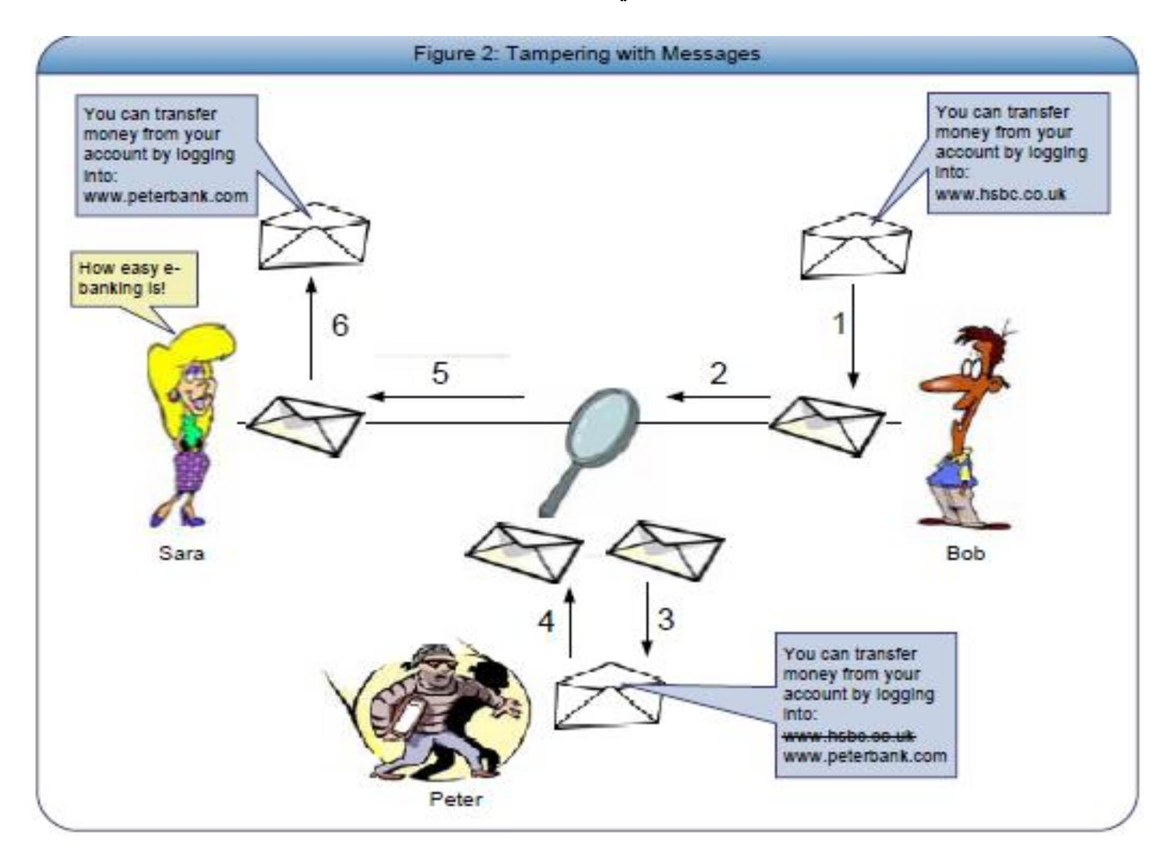
النسخة الانكليزية : الدكتور : محمد أنس طويلة – كندا –

لماذا نحتاج الى تشفير البيانات ؟

في أغلب الحالات ترسل البيانات عبر الشبكات الحاسوبية بشكل نص قابل للقراءة . بمعنى عند عملية إرسال البيانات من حاسب الى أخر عبر شبكة حاسوبية ما (مثل الانترنت غلى سبيل المثال), فان الشكل الأصلي للبيانات ترمز encoded وترسل عبر الشبكة كما هى . في هذه الحالة, الأشخاص السيئين المهتمين بسرقة معلوماتك يستطيعون سرقة البيانات التي ترسلها عبر الشبكة, وسيكون العقبة الوحيدة أمام فهم بياناتك التي أرسلتها هو فك ترميز الرسالة , في الحقيقة, هذا ليس عائق لان عملية ترميز البيانات لنقلها عبر الشبكات الحاسوبية هى عملية يقوم بها نظام التشغيل (مثل ويندوز) لكي يستطيع تنظيم البيانات لكي ترسل من حاسب الى حاسب عبر الشبكات . هذا خبر سيء! . لنرى المثال التالي الذي يوضح لماذا نحتاج الى التشفير. في المثال التالي (الشكل 1) , يريد Bob أن يرسل معلومات حساسة وخاصة (credit No.) الى Sara عبر الشبكة. يقوم بوب Bob بكتابة رسالته ويضع بياناته الخاصة فيها بشكل نصي صريح قابل للقراءة على أمل أن تقرأ فقط من قبل ساره Sara . بوب Bob تجاهل المخاطر المحتملة التي ربما يواجهها هذا النقل. الان, يوجد شاب سيئ النية يدعى بيتر Peter يتصنت على بيانات الآخرين ويستغلها في مصالحه الشخصية. فيقوم بيتر بمراقبة البيانات الحساسة التي يرسلها بوب Bob الى ساره Sara على أمل أن يجد شي مفيد , لان النص المرسل من بوب Bob الى ساره Sara هو نص صريح قابل للقراءة وبالتالي وبقليل جهد سيقرأ بيتر Peter كل البيانات المتبادلة.



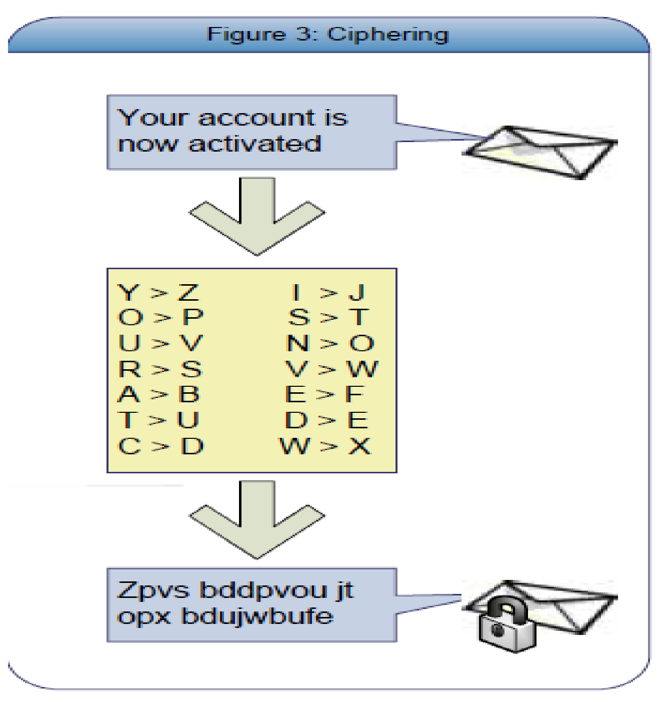
الخطر الأخر المرتبط بنقل البيانات الكترونيا عبر الشبكات, هو إمكانية تقليد شخصية المرسل. في المثال التالي (شكل 2), يستطيع بيتر Peter أن يقاطع الرسالة المرسلة من بوب Bob الى ساره Sara وان يغير في محتوى الرسالة ويعيد إرسالها الى ساره Sara والتي تعتقد سار أن هذه الرسالة هى من بوب Bob .



تشفير البيانات يستخدم لتقليل من مخاطر تعديل البيانات المرسلة عبر الشبكات, وأيضا جعلها خاصة وغير قابلة للقراءة من قبل الأشخاص السيئين الذين يسرقون البيانات . ويمكن للتشفير أيضا أن يمنع الأشخاص السيئين من انتحال شخصية المرسل عبر الشبكة .

كيف يعمل التشفير (التعمية) ؟

يستخدم التشفير في حماية البيانات الخاصة بتحويل الرسالة من شكل قابل للقراءة الى شكل أخر غير قابل للقراءة . لنفترض أن بوب Bob يريد أن يرسل الرسالة التالية الى ساره Sara : " حسابك تم تفعيله ". هذه الرسالة مكتوبة بنص صريح وقابل للقراءة ويستطيع أي شخص اعتراض الرسالة ويفهم ما قال بوب لساره. إذاً التخاطب بين بوب Bob وساره Sara ليس خاص بهما على أي حال. تنبه بوب لذلك وقرر استخدام التشفير لتحويل رسالته من نص مفهوم الى نص غير قابل للقراءة (يمكن فهم العملية مثل استخدام الطرود البريدية لتغليف الرسائل) . قام بوب باستخدام خوارزمية قيصر للتشفير Julius Caesar's cipher . الشكل-3 يوضح عمل هذه الإجرائية لتحويل النص الصريح clear text الى نص مشفر ciphered text . أصبح الان من الواضح أن أي شخص يعترض الرسالة المشفرة عبر الشبكة, سيكون من الصعب عليه فهم الرسالة المشفرة وبالتالي سيحافظ بوب على خصوصية قراءة رسالته الى ساره . لكن هل يمكن ان نقول ان رسائل بوب ستحافظ على خصوصيتها وسريتها في الوصول إليها؟ , في الحقيقة, سيكون من المستحيل القول بان النص المشفر لا يتعرض من عمليات فك التشفير decipher .



يسمى العلم الذي يدرس طرق كسر حماية خوارزميات التشفير " *Cryptoanalysis*" . المثال في الشكل- 3 – سهل الاختراق hacking , فخوارزمية التشفير عبارة عن عملية تبديل أحرف, فببذل جهد بسيط باستخدام الحواسيب الحديثة يمكن اختراق أي رسالة مشفرة بهذه الطريقة. توجد كثير من خوارزميات التشفير معقدة ومن الصعب اختراقها وكسر حمايتها. يجب عليك أن تتفهم أن التشفير لا يمكن أن يحمي بياناتنا للأبد. يمكن تعقيد خوارزميات التشفير في تعقيد زمن حساب احتمالات فك تشفير الرسالة المشفرة, وبالتالي ستفقد المعلومة قيمتها عندما يصل المخترق الى فك الرسالة الأصلية, طبعا التخطيط المناسب سيكون على عاتق الشخص الذي يريد أن يحمي بياناته.

إجرائية التشفير لديها مكونين رئيسين : خوارزمية التشفير ومفتاح التشفير. في طريقة تشفير Caesar المستخدم في المثال السابق , خوارزمية التشفير هى طريقة التبديل بين الأحرف substitution . فعندما يريد بوب أن يرسل رسالته الى ساره فعليه إخبار ساره انه سيستخدم خوارزمية قيصر في التشفير. والشيء الوحيد الذي يبقى خاص بين بوب وساره هو مفتاح التشفير, لان خوارزمية التشفير يمكن أن تكون معروفة و عامه.

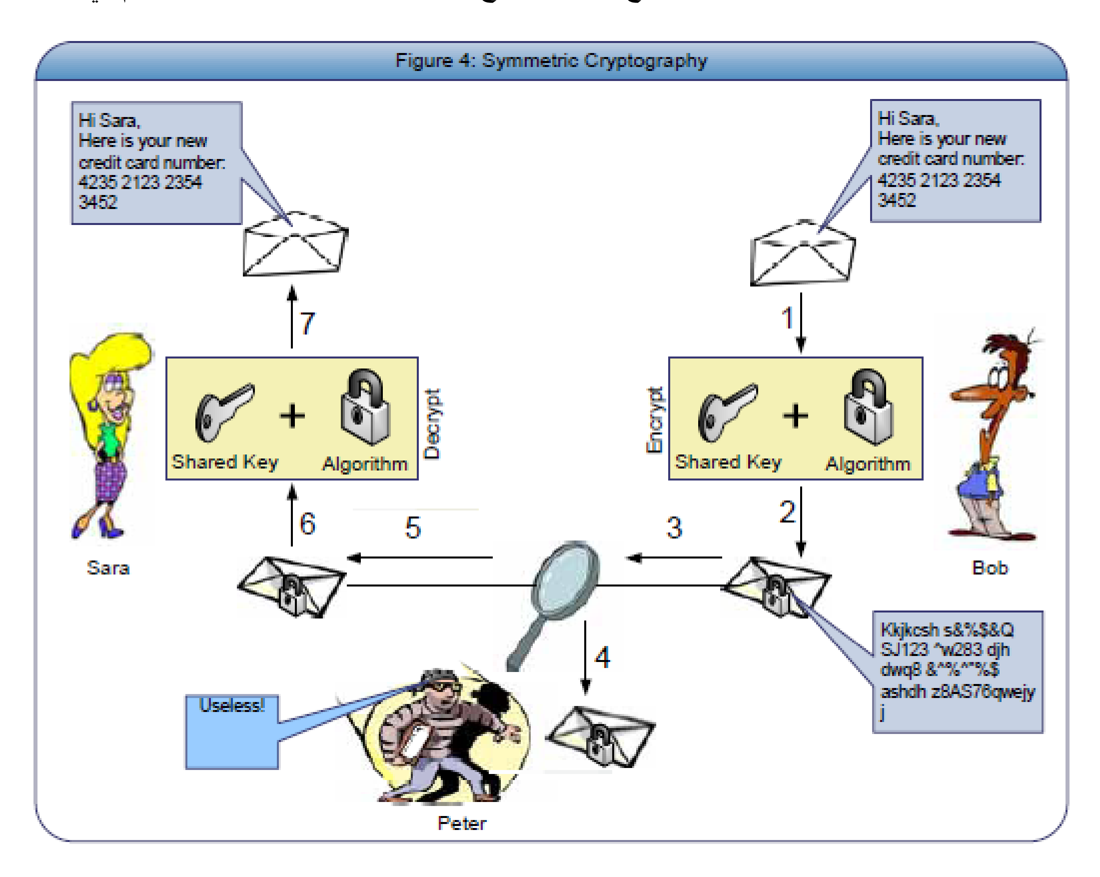
كيف يحمي التشفير بياناتنا ؟

يساعدنا التشفير على حماية بياناتنا و خصوصية اتصالانا الشبكية بعدة طرق, يساعدنا في :-

- تشفير الملفات على القرص الصلب أو أي وسيط تخزين وبالتالي الحفاظ على خصوصية بياناتك على حاسبك الشخصي على سبيل المثال.
- التوقيع الرقمي لمستنداتك وأيضاً البريد الالكتروني الخاص فيك لكي تستطيع التحقق من سلامة مستنداتك وبريدك الالكتروني ومنع الآخرين من انتحال شخصيتك أو تغير بياناتك أثناء نقلها على الشبكة.
- تشفير قنوات نقل المعلومات, مثل حماية قنوات النفاذ الى صفحات الويب أو الإجراءات البنكية.
- التحقق من صلاحية validity مستنداتك ورسائل بريدك الالكتروني , والسماح فقط للأشخاص المخولين Authorizing للوصول إليها فقط .

أنواع التشفير Type of Cryptography

كما أوضحنا سابقا, يتكون التشفير من جزأين رئيسين : خوارزمية التشفير ومفتاح التشفير. في أغلب الحالات تكون خوارزمية التشفير معروفة وعامة, في حين أن مفتاح التشفير يجب أن يحمى ويحفظ. لكي يستطيع طرفي الاتصال الاحتفاظ بخصوصية الاتصال بأمان يجب عليهما استخدام خوارزمية تشفير معروفة لكليهما وان يستخدما مفتاح التشفيرالمشترك بينهما, هذا النوع من التشفير يدعى بـ " **التشفير المتناظر Symmetric Cryptography"** , لان كلا المرسل والمستقبل يتشاركان بنفس خوارزمية التشفير ومفتاح التشفير في تشفير الرسائل بينهما وفك تشفيرها. الشكل- 4- التالي يوضح خطوات التشفير المتناظر. في هذا المثال حتى لو حاول بيتر Peter اعتراض الرسائل فهو لا يستطيع معرفة المفتاح المشترك بين بوب وساره المستخدم في التشفير.



كما نلاحظ أن التشفير المتناظر مبنى على أساس معرفة طرفي الاتصال المشفر بمفتاح التشفير المشترك بينهما. على سبيل المثال , إذا كان هناك شخص ثالث اسمه جاك Jack يريد أيضا إرسال رسالة مشفرة الى بوب, هو لا يستطيع عمل ذلك دون معرفة مفتاح التشفير لدى بوب. من الواضح أن على بوب أن يرسل مفتاح التشفير الى جاك لكي يستطيعان تشفير الرسائل وفك تشفيرها , لكن كيف يستطيع بوب توصيل المفتاح لجاك ؟, ماذا لو استطاع بيتر Peter اعتراض رسالة بوب والتي حتما يضع فيها مفتاح التشفير بنص صريح , وبالتالي سيتمكن بيتر من انتحال شخصية احد أطراف الاتصال وأيضا قراءة جميع الرسائل بين الأطراف المتبادلة. في حقيقة هذا السيناريو يضعنا أمام أهم مشاكل خوارزميات التشفير المتناظر !!! فما الحل إذاً ؟, البحث عن حل لهذه القيود أنتج طريقة أخرى في التشفير تدعى " التشفير الغير متناظر Asymmetric cryptography ".

التشفير الغير متناظر تم تطويره لحل مشاكل طريقة التشفير المتناظرة. في هذا النوع من التشفير, لا يستخدم مفهوم المفتاح المشترك, وعوضا عن ذلك, يستخدم مفهوم المفتاح العام Public Key والمفتاح الخاص Private Key . هذان المفتاحان مرتبطان بعملية التشفير وفك التشفير للمعلومات, كيف ؟. المعلومات تشفر بالمفتاح الخاص للمرسل ويفك تشفير المعلومات بواسطة المفتاح العام. بالإضافة الى ذلك يستطيع صاحب المفتاح الخاص أن يستخدم هذا المفتاح في التوقيع الرقمي , لان هذا المفتاح لا يمكن أن يكون عند شخص أخر. أيضا يستطيع المرسل أن ينشر مفتاحه العام لجميع الأطراف المتصل به عبر قناته المشفره, أما مفتاحه الخاص فيحتفظ به ليحافظ على خصوصية التوقيع الرقمي للمعلومات التي سوف تثق جميع الأطراف المتصل به أن هذه المعلومات هى حتما من الشخص المالك للمفتاح الخاص . إذاَ, دعنا نعود لمشكلة التشفير المتناظر, كانت المشكله هى كيف يستطيع بوب أن يرسل مفتاحه المشترك الى جاك. الحل هنا, وطالما هناك مفتاحان منفصلين فبإمكان بوب أن يرسل لجاك مفتاحه العام عبر أي وسيلة اتصال وسيحتفظ بوب بمفتاحه الخاص السري.

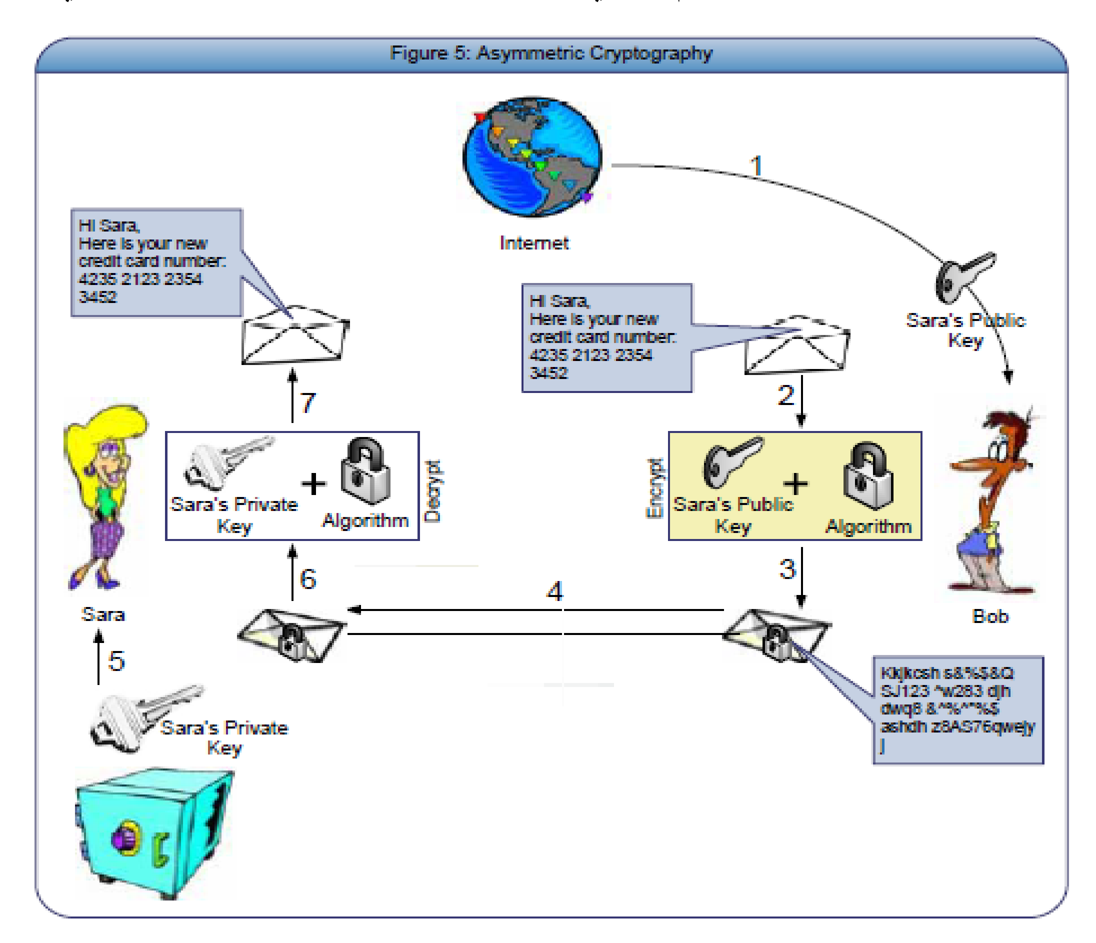


Figure 5: Asymmetric Cryptography

ويمكن نشر المفاتيح العامة hosting عبر الانترنت ضمن ما يعرف بالدليل العام(مثل دليل الهاتف) مثل PGP® وتقدم خدمة Global Directory للمفاتيح العامة[1]. ويمكن أيضا ان يرسل المفتاح العام بنص رسالة الى خدمة الدليل العام كما سنرى ذلك لاحقا في كيفية عمل ذلك. في الشكل- 5- السابق, أراد بوب تحسين مستوى الأمن في اتصالاته الخاصة مع ساره باستخدام التشفير الغير متناظر. قبل كل شي, ستقوم ساره بالبحث في دليل المفاتيح العمومية عبر الانترنت عن مفتاح بوب العام, ثم ستقوم بتشفير البيانات بمفتاح بوب العام وترسل البيانات الى بوب.

---

[1] لكي تستطيع نشر مفاتيحك العامه فيPGP ارجع للموقع التالي :
https://keyserver.pgp.com/vkd/GetWelcomeScreen.events

سيقوم بوب باستخدام مفتاحه الخاص (والذي يحتفظ به في مكان سري) في فك تشفير الرسالة المشفرة بمفتاحه العام . طبعاً, من المشاكل التي سيواجهها بوب باستخدام التشفيرالغير المتناظر هو السؤال التالي : أين المكان الآمن الذي سيحتفظ فيه مفتاحه الخاص ؟ , هذا السؤال يقودنا الى بناء بنية تحتية لتخزين المفاتيح تختلف عن بنية تخزين الملفات في أنظمة التشغيل, وبالفعل تم تطوير بنى ملفات خاصة بتخزين المفاتيح مثل PK#5 وغيرها, وسنتحدث بمثال عن ذلك عند التعرف على مشروع WinPT .

اذا, استخدام التشفير الغير متناظر مبنى على أساس إتاحة المفتاح العام للمشتركين معك في الاتصال الآمن في تبادل المعلومات مع الاحتفاظ لديك بمفتاحك الخاص أيضا. هذا يعني انه يتوجب عليك معرفة جميع المفاتيح العامة للأشخاص الذين تريد أن تصلهم رسائلك المشفرة وهذا يتطلب منك إدارة لتخزين المفاتيح العامة وسهوله التعامل معها في كل مره تريد التشفير. على سبيل المثال, لدى بوب ثلاثة أصدقاء ساره و جاك ومنى .استطاع بوب بطريقة ما معرفة المفاتيح العامه لكل أصدقائه. اذا فالمعلومات عند بوب كالتالي :

- المفتاح الخاص لبوب Bob .
- المفتاح العام لبوب.
- المفتاح العام لساره.
- المفتاح العام لجاك.
- المفتاح العام لمنى.

فعندما يريد بوب باستخدام البريد للالكتروني للتواصل مع جميع أصدقائه , فستزداد حجم معلومات التخزين لديه للمفاتيح العامة لجميع أصدقائه. فسيضطر بوب للبحث عن وسيلة لتسهيل وإدارة المفاتيح العامة لكي يستطيع بناء قنوات اتصال آمنه مع جميع أصدقائه. فوجد بوب أن الحل هو استخدام Public Key PKI – Infrastructure , و PKI طور لعمليات إدارة بنية المفاتيح(للتشفير الغير متناظر على سبيل المثال). في الفقرات التالية سنتعرف على مشروع WinPT والمصنف ضمن البرمجيات المفتوحة المصدر لنتعرف على كيفية استغلال هذه البنية التحتية في إدارة وتخزين مفاتيح التشفير.

القسم العملي : أدوات التشفير

في هذا الجزء من التطبيق العملي سنتحدث إن شاء الله عن أدوات إدارة المفاتيح في التشفير الغير المتناظر لتسهيل التعامل مع المفاتيح العامة وتنظيمها واستخدامها في التشفير وفك التشفير كما سنرى إن شاء الله تعالى .

سنتكلم عن أدوات برمجية مفتوحة المصدر تدعى Windows Privacy Tools (WinPT), وهي عبارة عن مجموعة من الأدوات تستخدم في التشفير الرقمي, تم إصدارها تحت ترخيص البرمجيات المفتوحة GPL[2]. الآن بإمكانك تنزيل آخر إصدارات النسخة من الموقع التالي:

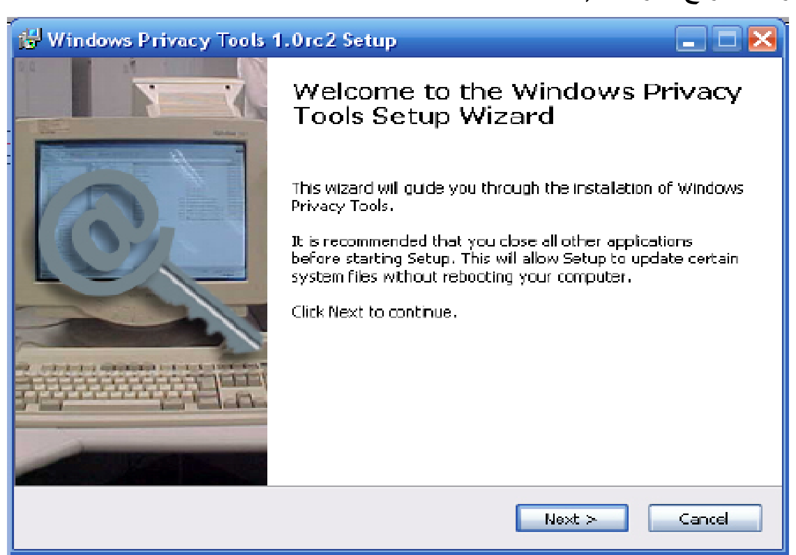
http:// winpt.sourceforge.net/en/download.php

1. **تنصيب WinPT**

بعد تنزيل النسخة من موقعها, اضغط ملف التنصيب , وسيظهر لك معالج خطوات التنصيب.
أولا, أختر اللغة التي تفضلها لقراءة خطوات التنصيب, ومن ثم اضغط على الزر "OK" .



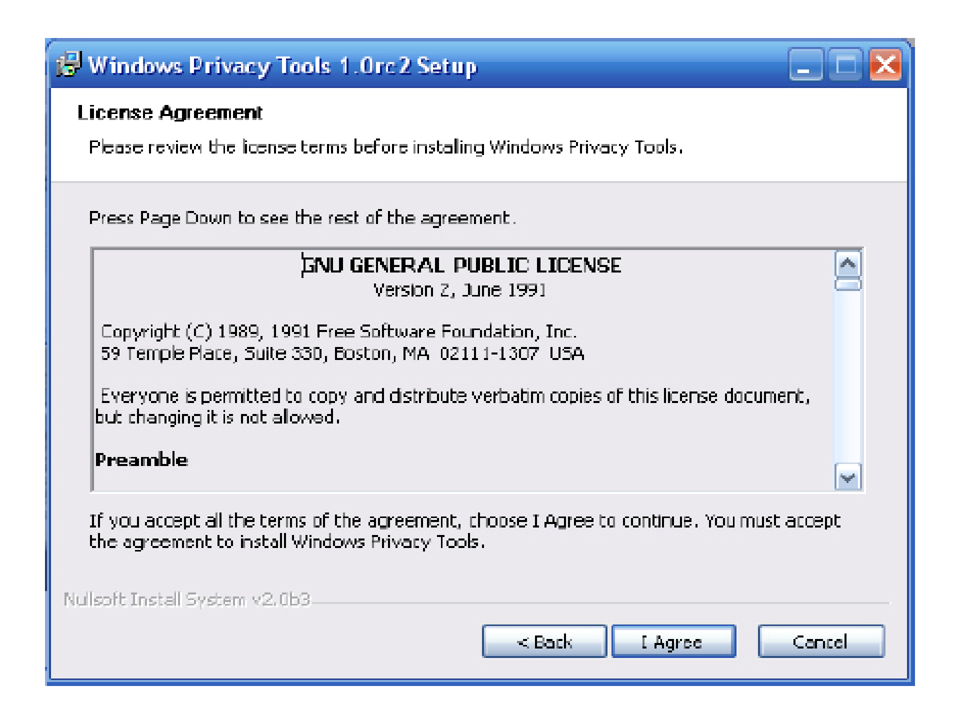
ستظهر لك مربع الترحيب, ببساطه اضغط "Next" .



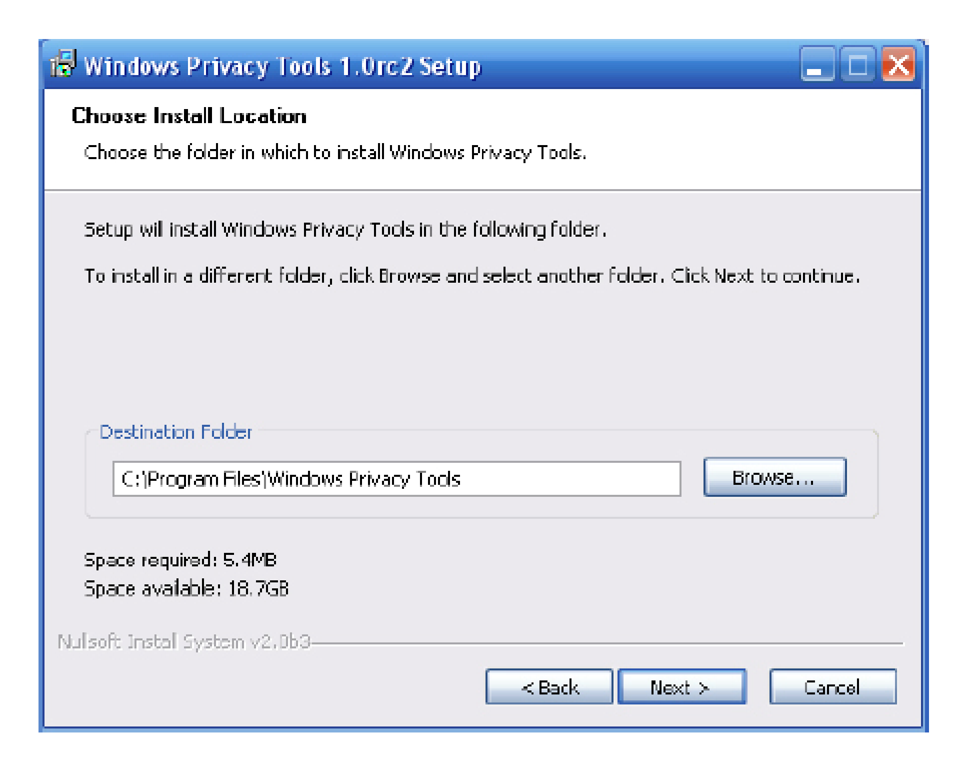
وبعد ذلك, سيظهر معالج التنصيب مربع يتضمن ترخيص استخدام هذه الأدوات. يجب عليك الموافقة على هذه الاتفاقية في استخدام هذه الأدوات . الشكل التالي اضغط على الزر"I agree" .

---

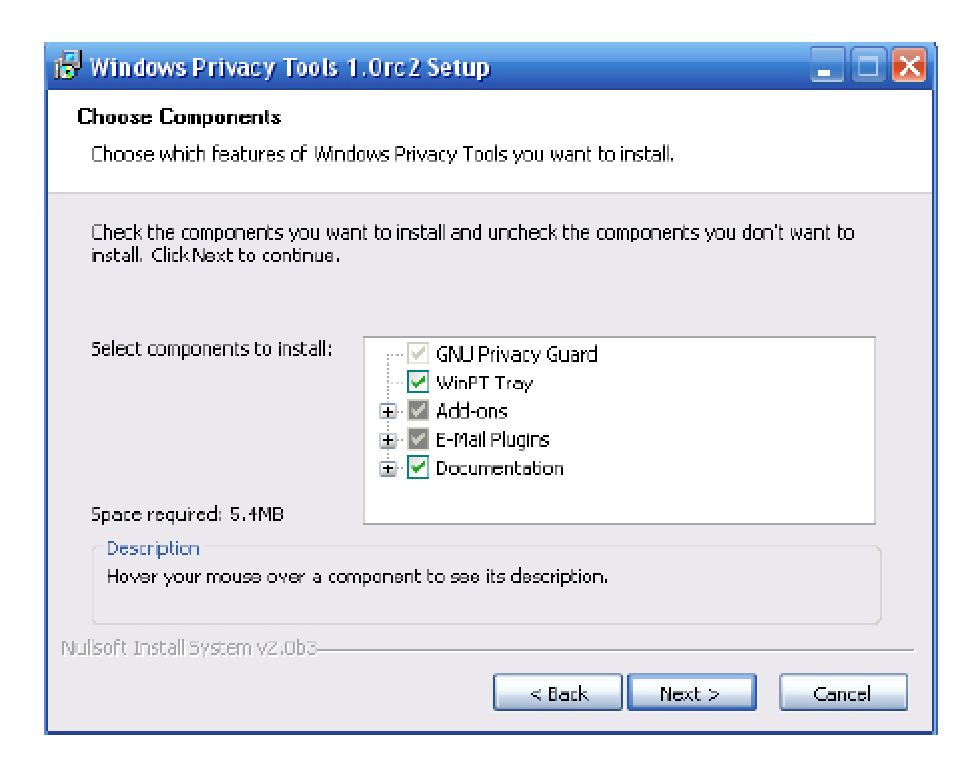
[2] GPL : اختصار لـــ GNU Public License . وجميع البرمجيات تصدر تحت مسمى Free Documentation License .



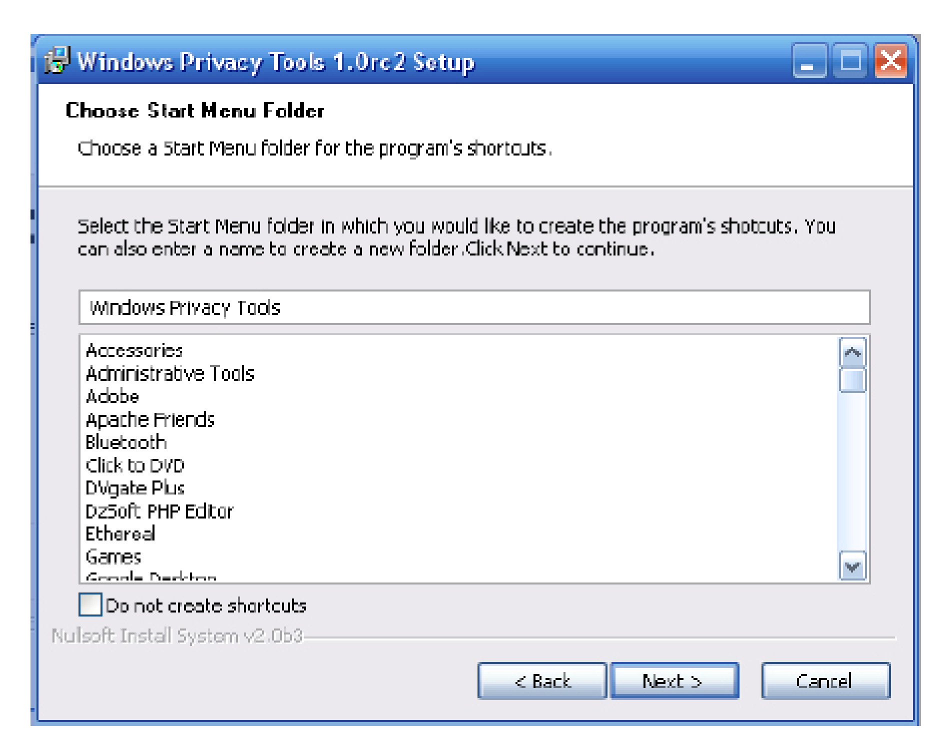
بعد الموافقة, سيظهر مربع تختار فيه مكان تنصيب هذه البرمجيات. يجب الانتباه جيدا للمساحة المتبقية من قرصك الصلب على حاسبك وأيضا مكان التنصيب. يجب أن يكون المكان خالي من الفيروسات حتى لا تتضرر ملفات الأدوات و هذا الأمر مهم جدا التنبه إليه. اضغط على الزر "Next" . كما يلي.



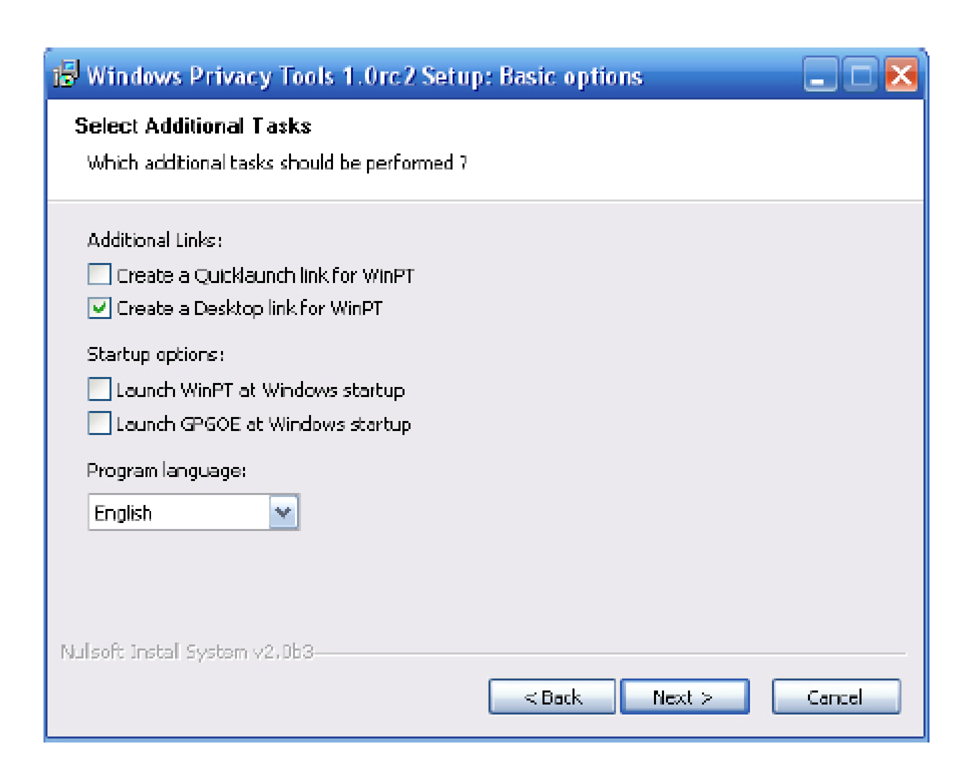
في الخطوة التالية, سيظهر لك مربع حوار تختار فيه المكونات التي ترغب في تنصيبها. على سبيل المثال, اضغط على الإعدادات الافتراضية واضغط على الزر " Next" :



المربع التالي , سيسألك إذا ما كنت تريد وضع قائمة الأدوات WinPT ضمن قوائم نظام التشغيل ويندوز. يمكنك اختيار أي قائمة تناسبك كما في الشكل التالي :

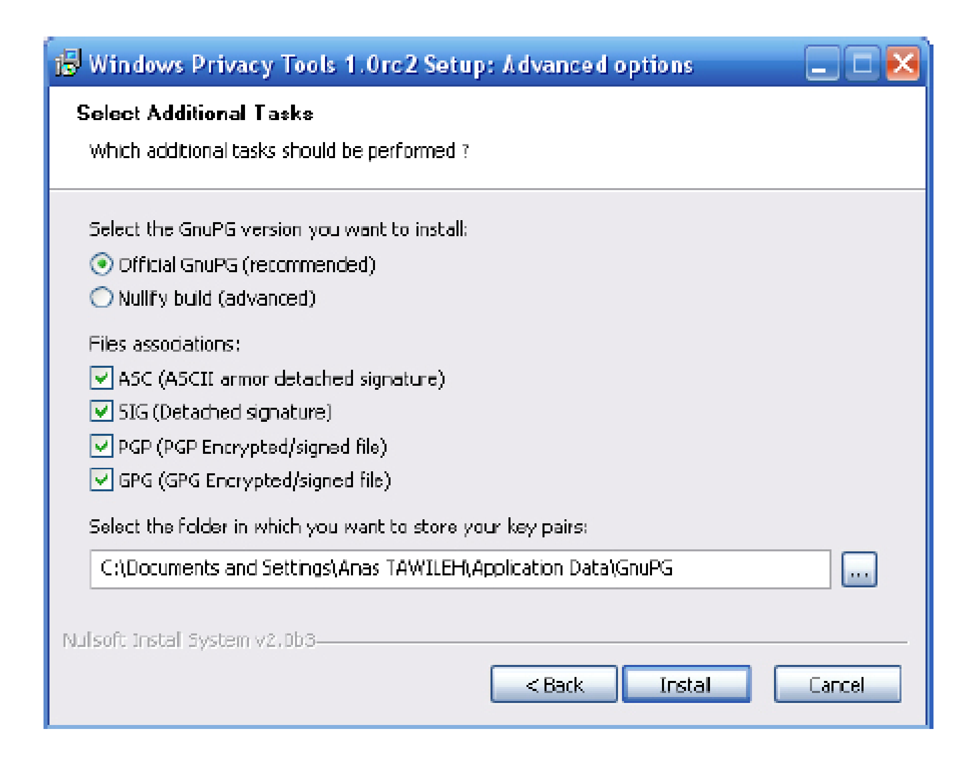


في الخطوة التالية, سيظهر لك مربع فيه خيارات كيفية إقلاع أدوات WinPT . على سبيل المثال اختيارك لـ start-up فكلما بدا تشغيل ويندوز سيقوم نظام التشغيل ويندوز بإقلاع أدوات WinPT . يمكنك اختيار ما يناسبك كما يلي:



الخطوة التالية, من أهم الخطوات في تنصيب أدوات WinPT بنجاح. قبل كل شيء, اختر نسخة GNUPG التي تريد استخدامها . ننصح بشده هنا باستخدام الإعدادات الافتراضية. إذا أردت تغير الخيارات الافتراضية يجب أن تكون صاحب معرفة بما تقوم به.

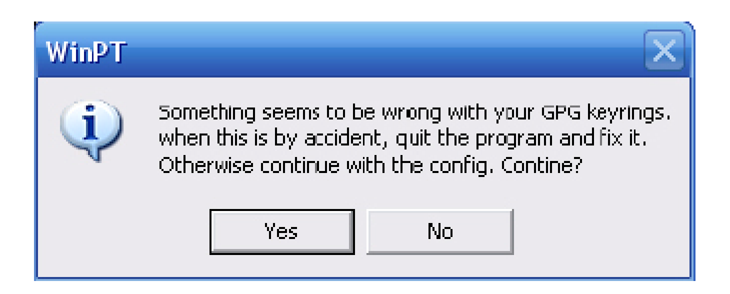
ثم اختر نوع الملفات التي تريد ربطها مع أدواتWinPT, والأكثر أهمية, اختر مجلد Directory لتخزين مفاتيح PGP. هنا يجب عليك أن تكون حذرا في اختيار المكان المناسب لهذا المجلد. لان وكما رأينا سابقا أن التشفير يحميك طالما حافظت على الخصوصية والسرية. وبعد الاختيارات اضغط على الزر 'install" . وستبدأ عملية التنصيب بعد دقائق .



2. التعامل مع إعدادات WinPT

لتشغيل أدوات WinPT, من قائمة ابدأ > جميع البرامج , windows Privacy Tools < WinPT Tray عند تهيئة البرنامج لكي يعمل, يقوم البرنامج بالبحث عن زوج المفاتيح المستخدمة في التشفير وفك التشفير . بالمفتاح الخاص يمكنك تشفير الرسائل التي ترسلها الى الآخرين, وأيضا بهذا المفتاح يمكنك فك تشفير الرسائل المرسلة إليك. ويمكنك أيضا استخدامه في التوقيع الرقمي لمستنداتك وبريدك الالكتروني. أما المفتاح العام, سيكون المفتاح الذي تنشره الى جميع الأطراف التي تريد أن تتبادل الرسائل المشفرة معهم, ويستخدم في تشفير الرسائل الى صاحب المفتاح الخاص المرتبط بهذا المفتاح وكذلك يستخدم في التحقق من المستندات أو البريد الالكتروني الموقع بالمفتاح الخاص المقابل له.

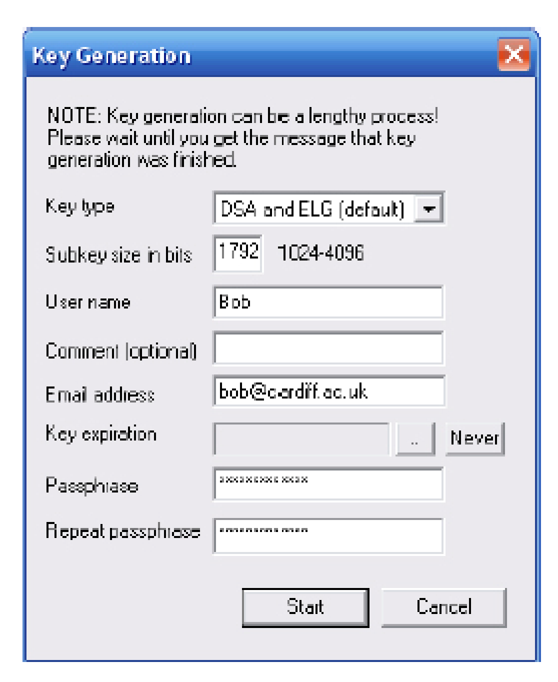
بسبب أن هذه أول مره لتشغيل أدوات WinPT , سيظهر لك مربع حوار تظهر فيه رسالة عدم القدرة على إيجاد زوج مفاتيح التشفير, وسيسألك إذا كنت تريد الاستمرار بالإعدادات للبرنامج. اختر "Yes"



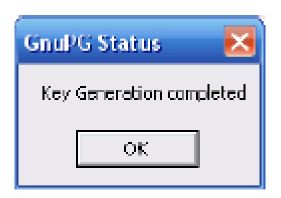
وطالما الى الآن لم ننشئ زوج المفاتيح الخاص بنا, سيظهر لك مربع فيه خيارات إنشاء هذان المفتاحان لك, يمكنك أيضا استيراد زوج مفاتيح من مكان ما اذا كان لديك مسبقا. اذا لم يكن لديك اي زوج مفاتيح ما عليك الا ان تضغط على الزر "OK" لتنشئ زوج مفاتيح خاص فيك.



سيظهر لك مربع حوار, اختر نوع خوارزمية توليد أزواج المفاتيح التي تريدها (يمكنك استخدام الاعدادات الافتراضية DSA: و ELG), حجم جزء المفتاح المطلوب (طبعا كلما كان اكبر كان الامان أكثر, وهذا سيكون على حساب زمن توليد زوج مفاتيح التشفير), وأيضا ادخل معلومات عنك (لسهولة تحديد هوية المفاتيح وتذكرها للتعامل معها). ويمكنك ايضا تحديد تاريخ صلاحية لزوج المفاتيح المراد توليدها. أخيرا, اكتب كلمة سر Passphrase التي تريدها مرتين. أرجو أن تختار كلمة سر معقدة نوعا ما, مثلا تتضمن أرقام وأحرف وأحرف خاصة وما شابه ذلك لزيادة التعقيد في خصوصية زوج المفاتيح, وينصح أن تكون عموما اكبر من 10 أحرف . حاول أن تتجنب استخدام كلمات سهلة التخمين أو موجودة في القواميس (مثلا تاريخ ميلادك , اسم مفضل لديك وما شابه ذلك). اضغط الآن على "start" . وكن صبورا ريثما يتم توليد المفاتيح .



وعند اكتمال توليد المفاتيح سيظهر لك المربع التالي :



الجدير بالذكر هنا, يجب عليك بشده الحفاظ على المفاتيح المولدة, لأنه في حال فقدانك لها لا يمكن استرجاعها . لذا ستظهر لك رسالة تنبهك بهذا الأمر , وتتيح لك خيار إذا ما كنت تريد عمل نسخة احتياطية لزوج المفاتيح المولده, وايضا هنا يجب الانتباه ان مكان النسخة الاحتياطية يجب ان يكون محمي أيضا.



تهانينا!, لقد تم العمل بنجاح في إعداد WinPT ويمكنك الان الانتقال معنا الى الخطوة التالية في كيفية التشفير وفك التشفير كما سنرى ذلك.

3. استخدام WinPT

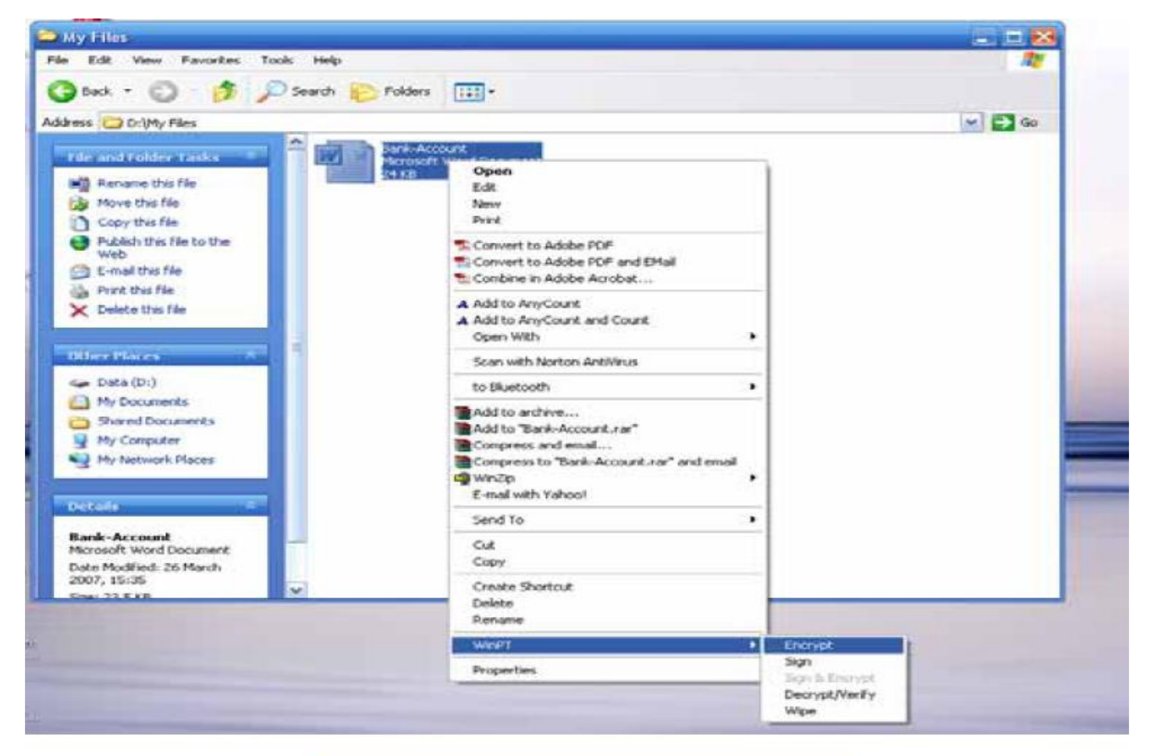
التشفير باستخدام أدوات WinPT :

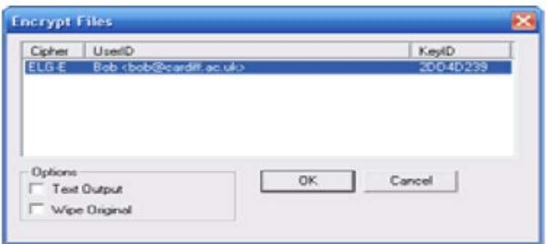
الان بعد إتمام عملية التنصيب والإعداد , يمكنك استخدام أدوات WinPT في تشفير أي ملف تريد أن تجعله محمي. قبل البدء بشرح طريقة التشفير, ارجوا أن تتأكد أن برنامج WinPT تشتغل كما في الصورة التالية .



تشفير الملفات باستخدام WinPT سهل جدا ومباشر. من قائمة windows explorer حدد الملف الذي تريد أن تشفره. اضغط الزر الأيمن للماوس على أيقونة الملف المراد تشفيره, ومن القائمة المنسدلة اختر WinPT . ستجد عدة خيارات تختار منها ما تريد عمله. الشكل التالي يوضح ذلك. وفي مثالنا اختر تشفير الملف, وسنركز على بقية الخيارات مؤخرا.

بعد الضغط على الخيار "Encrypt". سيكون عليك أن تقرر من الذي يستطيع فك تشفير ملفك , و هذا عن طريق تحديد من الذين يملكون المفتاح العام المقابل للمفتاح الخاص الذي قمت بتشفير الملف به. أيضا باستخدام WinPT يمكنك فك تشفير الرسالة المرسلة إليك عن طريق تحديد المفتاح الخاص المقابل للمفتاح العام الذي تم تشفير الرسالة به. ولما كان هناك عده مفاتيح عامه, سيقدم لك WinPT بكل سهولة مربع حوار لتختار المفتاح العام للتشفير. انظر الشكل التالي. ثم اضغط على الزر "OK" .

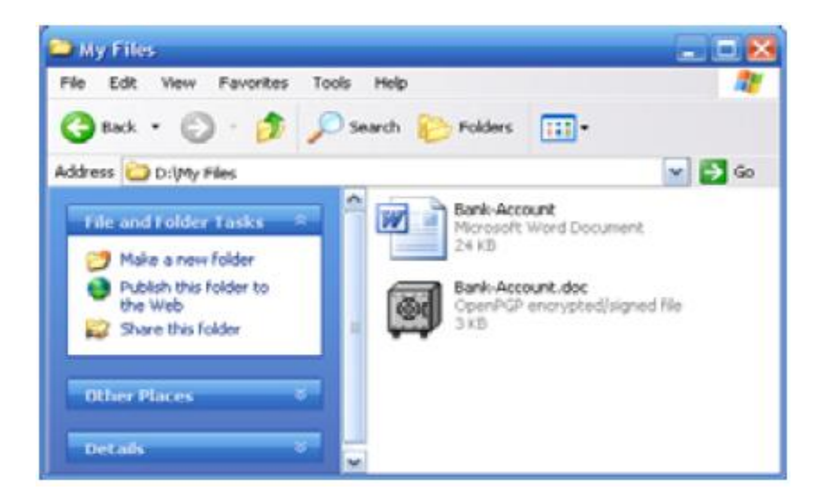




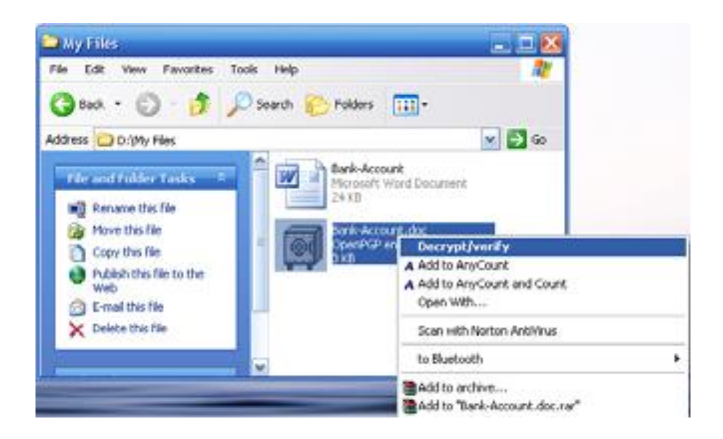
بعد أن يقوم WinPT بتشفير الملف, سيكون اسم الملف بعد التشفير بالصيغة التالية:

<Original-File-Name>.gpg

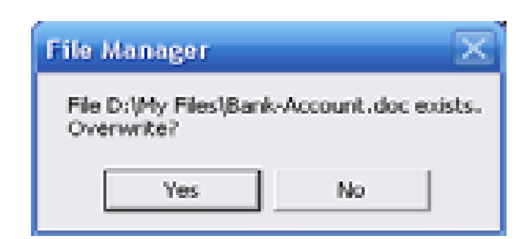
في الشكل السابق, إذا اخترت "Wipe Orginal" , سيقوم WinPT بتدمير[3] الملف الأصلي بعد أن يتم تشفيره . وبالتالي فلا توجد أي طريقة لاستعادة الملف الأصلي إلا بفك تشفير الملف المشفر المقابل للملف الأصلي. انظر الشكل التالي.



لفك تشفير الملف, بكل بساطه اضغط على الملف المشفر بالزر الأيمن للماوس, واختر "Decrypt/Verify".



إن لم تحذف الملف الأصلي على نفس المجلد, سيظهر WinPT رسالة تنبهك بوجود نفس الملف . اضغط للموافقة على عملية إعادة الكتابة عليه .



[3] طبعا, قد تسال هل باستخدام برامج استعاده الملفات , يمكن استعاده الملف الاصلي ؟؟؟, اظن ان البرنامج يستخدم طريقة جيده في تدمير الملفات يصعب استرجاعها بسهولة!!!!!.

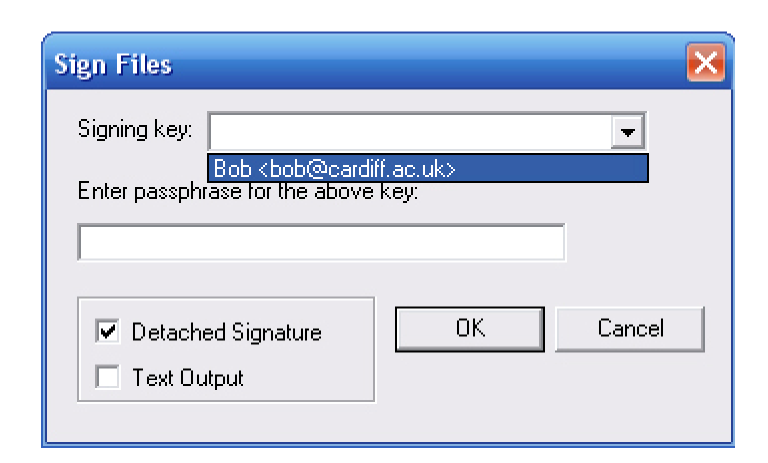
وفي هذه الحالة, ستطالب بإدخال كلمة السر Passphrase للوصول للمفتاح الخاص لفك تشفير الملف. ادخل كلمة السر ثم اضغط على الزر "OK" .



التوقيع الرقمي للملفات

توقيع الملف يعني انك تؤكد وتثبت للمرسل أن هذا الملف هو الملف الأصلي منك وليس من شخص ينتحل شخصيتك . عند توقيع الملف , فان مفتاحك الخاص سيستخدم في التوقيع الرقمي (نص صغير مشفر). والتوقيع الرقمي يُمَكن المستقبل من التحقق من هوية المرسل باستخدام المفتاح العام. وبما انك الشخص الوحيد الذي يمتلك المفتاح الخاص, فمن المستحيل لأي شخص غيرك أن يزور توقيعك . يمكن أن تضع التوقيع الرقمي مع الملف الموقع , أو يمكن إرساله عبر ملف منفصل, أو أي طريقة تفضلها. والأمر يعود لسياستك الأمنية.

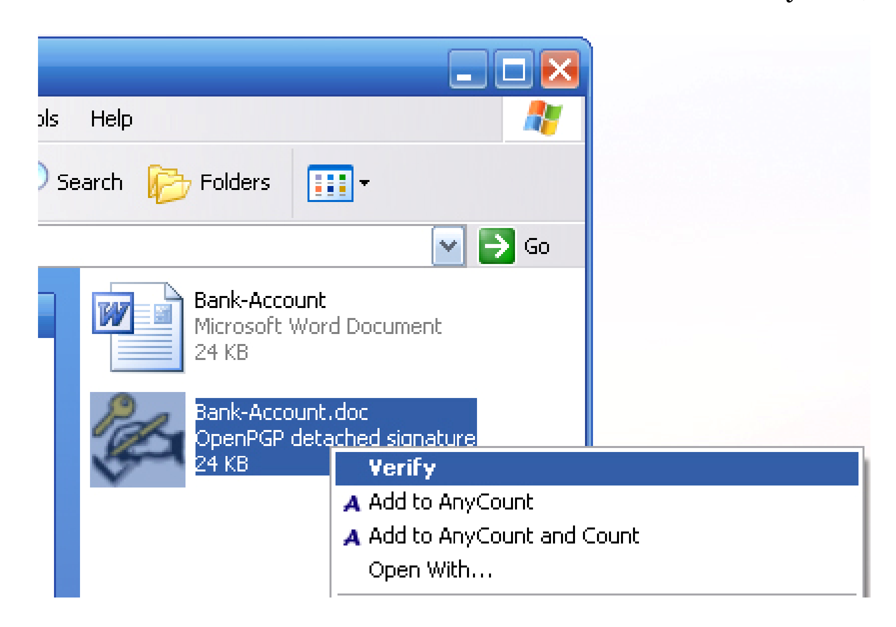
لتوقيع ملف, زر يمين بالماوس ثم اختر "Sign" . ستسال عن المفتاح الخاص الذي تريد بتوقيع الملف. اختر المفتاح المناسب (هنا عن طريق الايميل الذي أدخلناه في مرحلة التهيئة ل WinPT). وستطالب أيضا بإدخال كلمة السر (المرتبطة بهذا المفتاح عند إنشاءه). ثم اختر طريقة تخزين التوقيع ضمن ملف منفصل على عن الملف الأصلي. اذا لم تختر أي من خيارات تخزين الملف فان التوقيع يخزن في الملف الأصلي. ثم اضغطOK



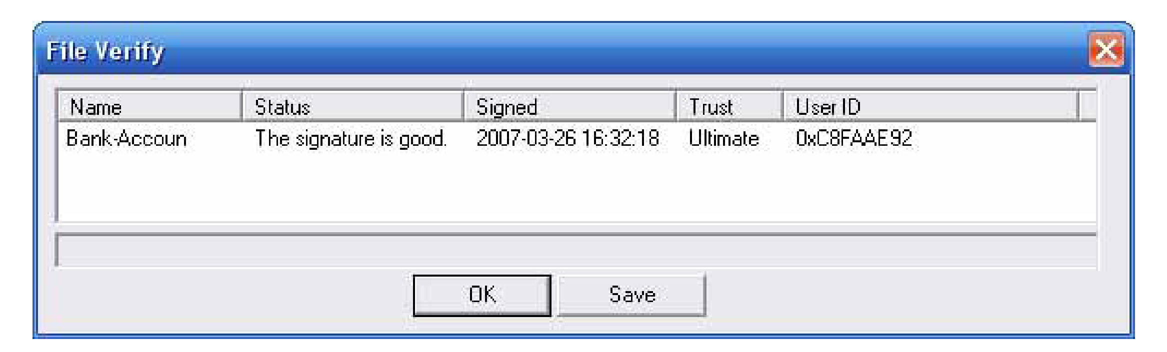
سيقوم WinPT بتوليد ملف يتضمن التوقيع الرقمي وسيكون اسم ملف التوقيع بالشكل التالي:

<original-file-name>.sig

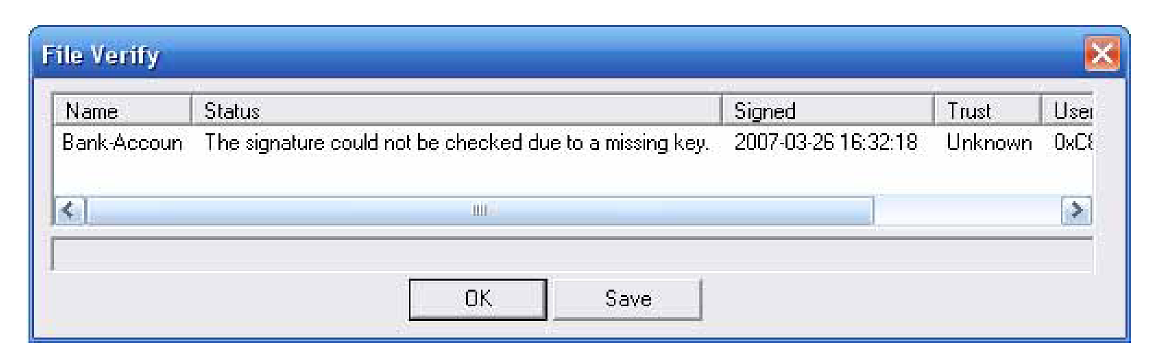
انظر الشكل التالي. ويمكنك ان تتحقق من التوقيع من خلال الملف الموقع بالضغط زر يمين بالماوس على ملف التوقيع ثم اختر "verify" .



فعندما تتحقق من التوقيع, سيظهر لك مربع حوار لتحديد المفتاح العام . فإذا نجح التحقق من التوقيع الرقمي ستظهر الرسالة كما في الشكل التالي , والتي هى عبارة عن معلومات عن الموقع.



إذا فشل التحقق من التوقيع الرقمي ستظهر الرسالة كما في الشكل التالي:

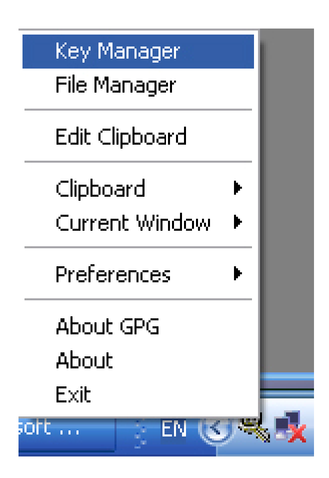


تشفير البريد الالكتروني

قبل أن نبدأ بتعلم كيفية تشفير البريد الالكتروني, يتوجب عليك تجميع المفاتيح العامة لكل شخص تريد أن ترسل إليه الرسائل المشفرة. بالإضافة لذلك, يجب أن تكون متأكدا أن مستقبلي رسائلك المشفرة لديهم مفتاحك العام كي يستطيعوا أيضا فك تشفير رسائلك الخاصة إليهم.

لنبدأ الان بتناول كيفية نشر مفتاحك العام للأشخاص الذين تريد أن تتواصل معهم برسائل مشفرة. أولا, سيكون اتخاذ قرارا كيف ذلك يعود الى سياستك الأمنية. تستطيع أن تنشر مفتاحك العام يدويا عن طريق البريد الالكتروني, أو عن طريق قرص صلب CD-ROM , و الذاكرة الخارجية USB Memory . في الحقيقة, هذه المرونة ناتجة عن عدم وجود أي مخاطر مرتبطة بتوزيع المفتاح العام. لكن ذلك باستخدام الطريقة اليدوية في نشر المفتاح العام سيجعل عدد الأشخاص الذين تتواصل معهم محدود . الطريقة الأخرى التي يمكن أن تنشر المفتاح العام كما أسلفنا سابقا عن طريق دليل المفاتيح العامة (PGP® Global Directory) ويمكن الوصول إليه عن طريق الموقع: https://keyserver.pgp.com/vkd/GetWelcomeScreen.event .

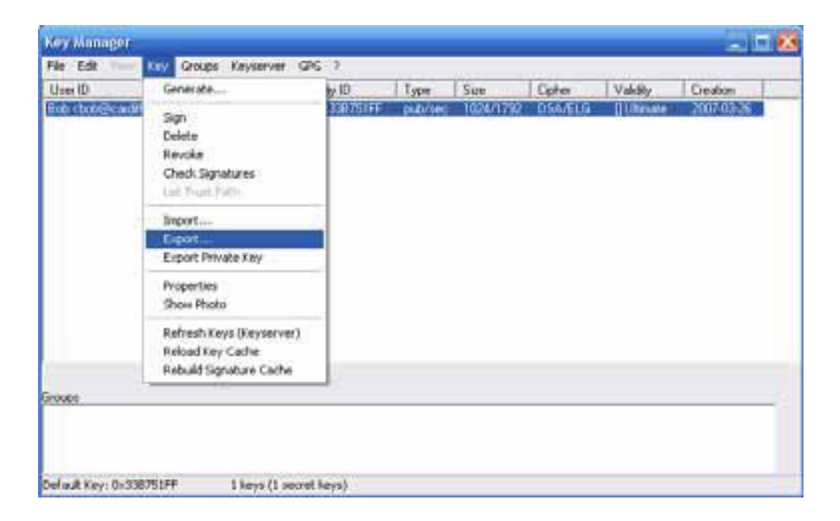
عندما تنشر مفتاحك العام عن طريق خدمة الدليل العام عبر الانترنت, أي شخص يريد استخدام تشفير الرسائل إليك, سيتوجب عليه أن يبحث في هذا الدليل عن المفتاح العام الخاص بك, ويقوم بتنزيله ويضيفه الى مجلد التخزين للمفاتيح عن طريق أدوات WinPT . وبالتالي يستطيع أن يرسل لك الرسائل المشفرة بالمفتاح العام. وبنفس الطريقة يمكنك أن تبحث عن المفاتيح العام لأي شخص ترغب في إرسال اليه رسائل مشفره باستخدام مفتاحه العام. لتضمين المفتاح العام الذي حصلت عليه من الدليل العام من الانترنت. اضغط زر يمين بالماوس على ايقونة WinPT الظاهرة أسفل الشاشة كما في الشكل التالي:



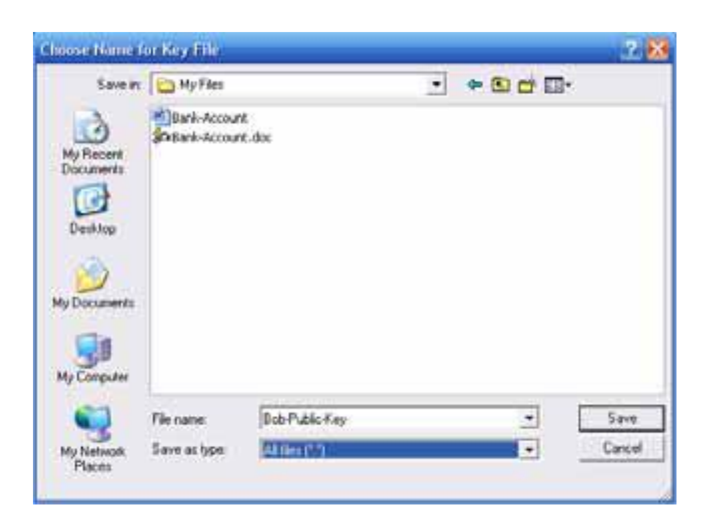
توفر WinPT خدمة مدير المفاتيح Key Manager : وهو المسئول عن إدارة المفاتيح في WinPT . عن الدخول الى مدير المفاتيح سوف تشاهد جميع المفاتيح الخاصة والعامة التي تستخدمها في التشفير وفك التشفير ايضا. اضغط على المفتاح العام ثم بالزر الأيمن بالماوس على المفتاح العام ثم تصدير export [4] اذا رغبت بنشر مفتاحك العام على دليل خدمة المفاتيح العامه كما أسلفنا. في الشكلين التالين ستتعرف على طريقة تصدير مفتاحك العام من منصة WinPT الى ملف خارجي لتضعه على خدمة الدليل العام على الانترنت.

---

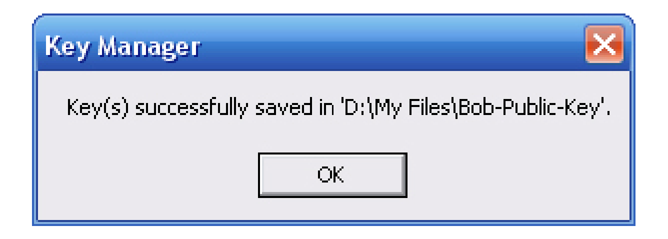
[4] انتبه !! احذر ان تصدر مفتاحك الخاص.



ستسال هنا باختيار مكان حفظ الفتاح العام, كما يلي:

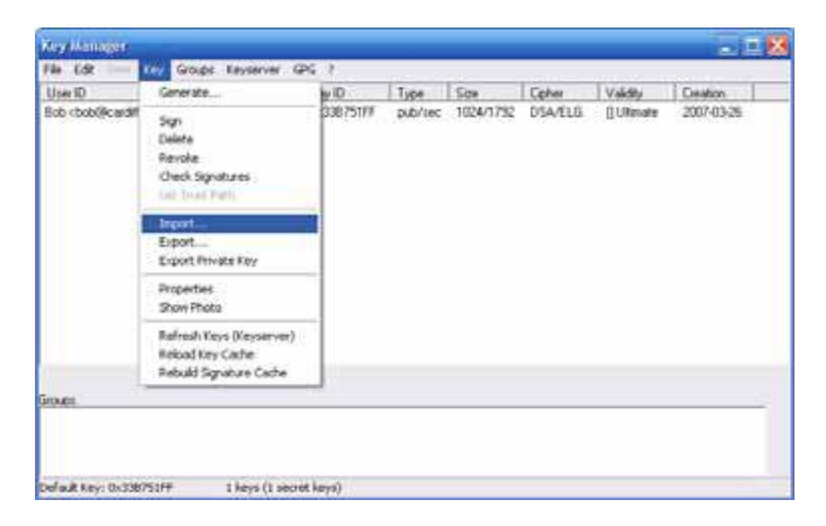


اخيرا, سياكد لك WinPT نجاح العملية .



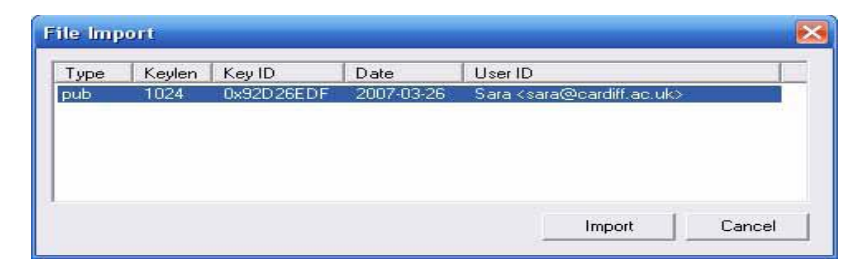
الان, إذا رغبت بتضمين import المفاتيح العامة لأصدقائك لتعمل ضمن منصة WinPT . بكل بساطة يمكنك عمل ذلك. ادخل الى Key Manager كما أسلفنا سابقا, ومن ثم اضغط على Key من شريط القوائم, ومن ثم اضغط import من القائمة المنسدلة. كما في الشكل التالي.(و هنا يجدر الملاحظة أن المفتاح العام الذي سوف تضمنه في WinPT يجب أن يكون على ملف نصي TXT).

بعد اختيار ملف المفتاح العام اضغط على Open .



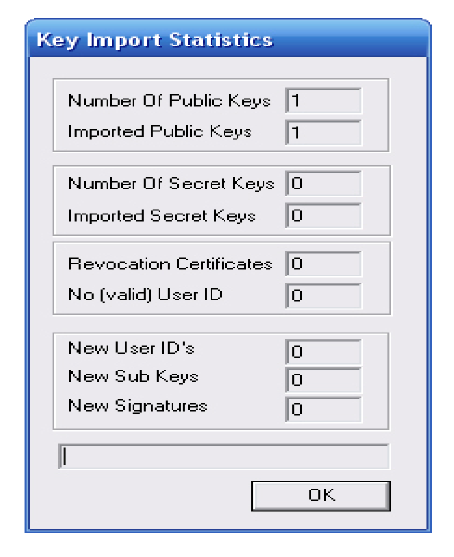


وبعد ذلك, ستظهر لك قائمة بكل المفاتيح العامة الموجودة ضمن الملف, اختر اسم المفتاح الذي ترغب بتضمية. انظر الى الشكل التالي.



وبعد ذلك ستظهر لك قائمة إحصائية عن عدد المفاتيح العامة التي تم تضمينها بنجاح. خذ نظره على هذه القائمة ثم اضغط "OK" .

وبالتالي سيكون قد انتهيت من تضمين مفاتيح أصدقاءك العامة الى منصة عمل WinPT , ويمكنك الآن إرسال الرسائل عبر البريد الالكتروني بشكل مشفر.



الان, لنرى كيف سنستخدم تشفير البريد الالكتروني. من الأخبار الجيدة التي يمكنني أن أخبرك بها, هي أن منصة عمل WinPT هو plug-in على نوعين من برامج التعامل مع البريد الالكتروني هما: البرنامج الشهير للتعامل مع البريد الالكتروني Microsoft Outlock Express وبرنامج .Eudora . عند فتح احد البرنامجين السابقين ستلاحظ وجودة أيقونه صغيره ضمن قوائم البرنامج .

ملاحظة هامة: قبل أن تبدأ في استخدام Outlock, تأكد أن plug-in loader يعمل(انظر الشكل التالي). إذا لم يكن يعمل اذهب الى مجلد (تماما الى (GPGOE تنصيب WinPT واضغط على الملف GPGOEInit.exe. يجب أن يكون المشهد عندك كما في الشكل التالي:

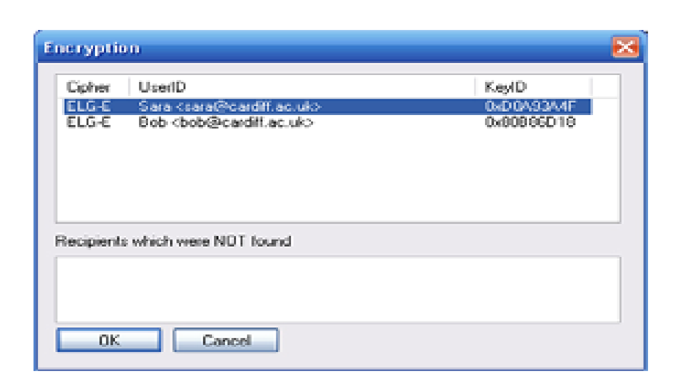


الان, أصبحنا جاهزين لإرسال البريد الالكتروني المشفر. بعد الانتهاء من كتابة نص رسالتك, اضغط على أيقونة Encrypt كما في الشكل التالي.



إشارة القفل في الشكل السابق, تشير أن الرسالة ستشفر. ثم اضغط على "Send" .

سيظهر لك مربع يطلب منك تحديد المفتاح العام المراد تشفير الرسالة به. اختر المفتاح العام الذي ترغب به, ثم اضغط على الزر "OK" .



الان, يكون قد أرسلنا البريد الالكتروني المشفر. كيف الان نفك تشفير البريد الالكتروني؟؟؟؟

بكل بساطة, افتح برنامج Microsoft outlock ثم افتح الرسالة المراد فك تشفيرها, اضغط على أيقونة فك التشفير "decrypt", لاحظ البرنامج سيطلب منك إدخال كلمة السر المرتبطة بالمفتاح الخاص المقابل للمفتاح العام الذي شفر هذه الرسالة.

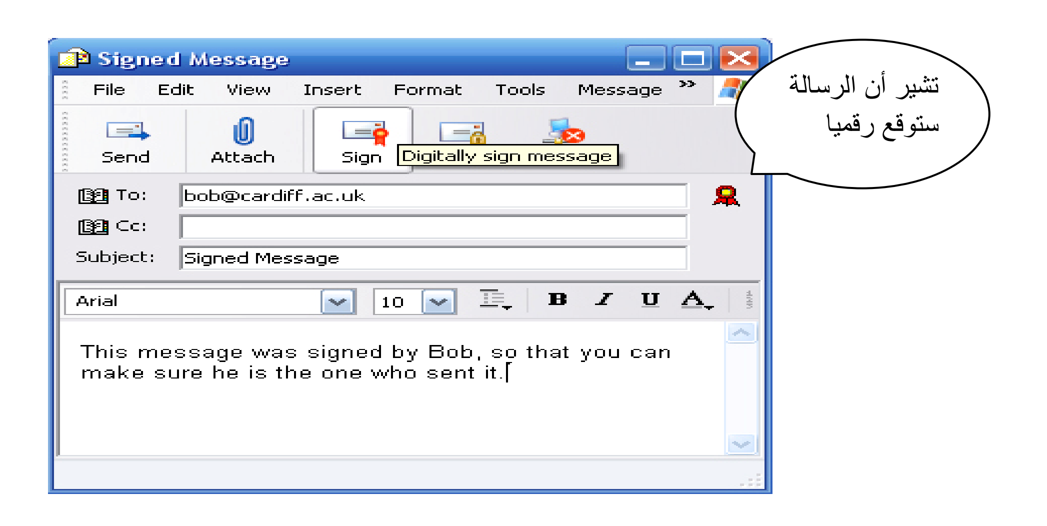


بعد التحقق من انك مالك للمفتاح الخاص من خلال كلمة السر التي قمت بإدخالها سيظهر المفتاح الخاص المقابل للمفتاح العام الذي شفرت به هذه الرسالة, وبالتالي سيمكنك قراءة الرسالة المشفرة. وتهانينا لك على الانجاز.

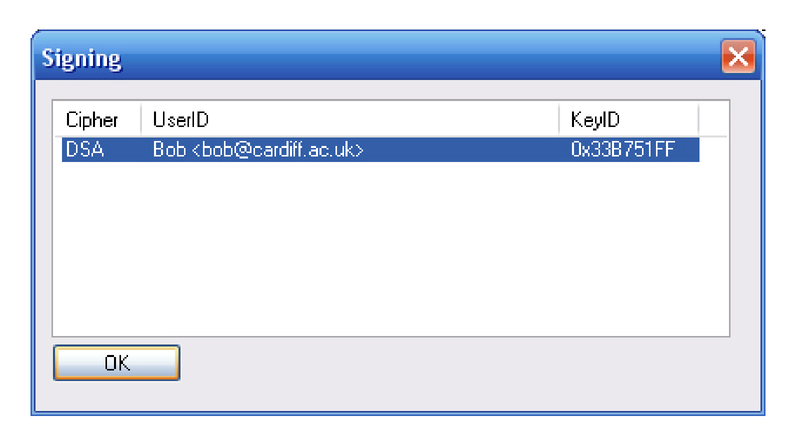
توقيع البريد الالكتروني

يستخدم التشفير بالمفتاح العام والمفتاح الخاص (او تسمى التشفير بالمفتاح العام اختصارا*) في تحقيق مفهوم المصادقة أو التوثيق Authenticity للمعلومات, بالإضافة الى الحفاظ على سريتها. يمكن تحقيق التوثيق باستخدام التوقيع الالكتروني كما رأينا سابقا سواء على الملفات أو البريد الالكتروني.

لنرى الان كيف عمل توقيع البريد الالكتروني. لتوقيع البري الالكتروني باستخدام مفتاحك الخاص كما رأينا سابقا. أولا, اكتب نص رسالتك البريدية ثم اضغط على أيقونة "Sign" في شريط القوائم. كما في الشكل التالي.



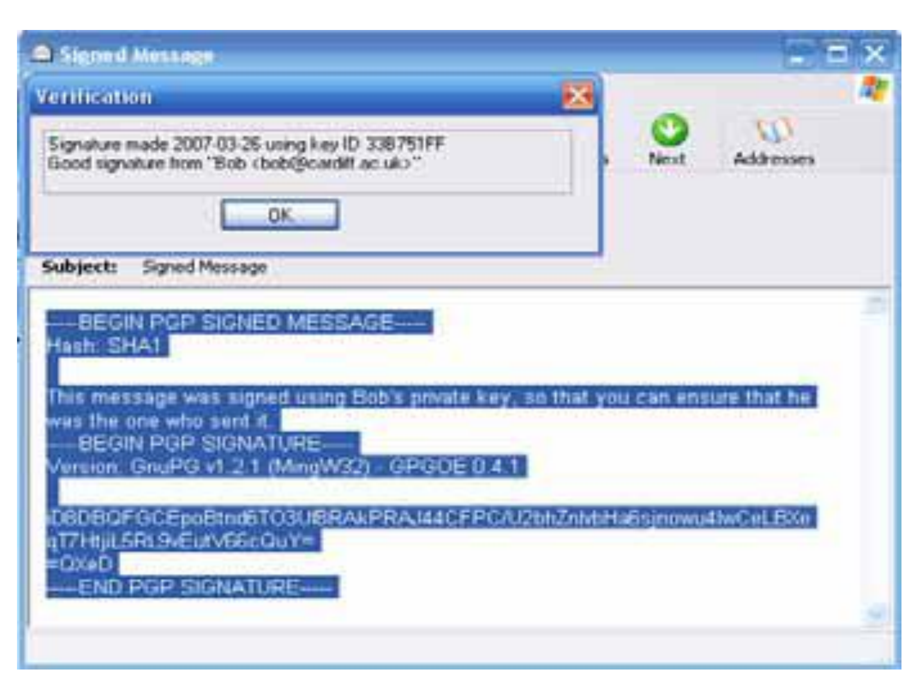
بعد الضغط على "Send" , سيظهر لك المربع التالي والذي يظهر قائمة بالمفاتيح الخاصة التي لديك والتي ستستخدم احدها في عملية التوقيع الرقمي. اختر احد المفاتيح ثم اضغط على "OK" .



سيظهر لك مربع لتدخل كلمة سر للوصول الى مفتاحك الخاص والذي تحتفظ به. ادخل كلمة السر المتعلقة بمفتاحك الخاص ثم اضغط على الزر "OK" .



الان, لنرى كيف تتحقق من توقيع (التوثيق Authentication) رسالة استلمتها من احد أصدقاءك. أولا يجب ان يكون لديك المفتاح العام المرتبط بالموقع على الرسالة التي استلمتها. يمكن الوصول الى المفتاح العام لشخص كما أسلفنا سابقا. الان عندما تستلم الرسالة الموقعة من شخص ما, قم بفتحها باستخدام برنامج البريد الالكتروني Outlook . الان, اضغط على ايقونة "verify" وسيقوم برنامج WinPT بمقابلة المفتاح العام المضمن ضمنه . فاذا نجح التحقق سيظهر WinPT لك رسالة تأكيدية توضح نجاح عملية التحقق.



كملاحظة أخيره: تذكر أن استخدامك للتشفير والتوقيع سيؤمن ذلك عمليتي الحفاظ على سرية البيانات وأيضا عملية التوثيق, وهذا يزيد من مستوى الأمن.